Claims

1. A method for creating a computer identifier for an online customer for detecting a possible fraudulent transaction in the course of an online transaction comprising the steps of:

receiving, from said customer's computer, at least one personal or non-personal identification parameter;

capturing, from the clock of said customer's computer, said customer's computer local time;

capturing, from a website's server clock, said server's local time;

creating and storing a delta of time parameter based upon the difference between said customer's computer local time and said server's local time; and

uniquely identifying said customer with said delta of time parameter and said at least one personal or non-personal identification parameter.

2. The method of Claim 1 further including the step of receiving, from said customer, an additional identification parameter comprising personal identification information relating to said transaction.

3. The method of Claim 1 wherein said at least one non-personal identification parameter is said computer's IP address.

4. The method of Claim 1 wherein said at least one non-personal identification parameter is said computer's Browser ID.

5. The method of claim 1 wherein said delta of time parameter is stored as a range of time.

6. A method for detecting fraud in an online transaction by a customer comprising the steps of:

creating a first computer identifier in the course of an online transaction comprising the steps of Claim 1;

creating at least a second computer identifier in the course of a second proposed online transaction comprising the steps of Claim 1;

utilizing a matching parameter to compare said first computer identifier with said second computer identifier;

creating a matching value based on the similarities between said first computer identifier and said second computer identifier; and

classifying said second online transaction as fraudulent, not fraudulent, or requiring further consideration based upon the value of said matching parameter.

7. The method in Claim 6, further comprising:

communicating to the website operator an indication, as to whether said second online transaction is fraudulent, not fraudulent, or requires further consideration.

8. The method in Claim 6, further comprising:

blocking said second online transaction based upon the value of said matching parameter.

9. The method in Claim 6, further comprising:

communicating to said customer the status of said second online transaction based upon the value of said matching parameter.

10. The method in Claim 6, wherein said delta of time parameter is stated as a range of time.

11. The method of claim 6 wherein said personal or non-personal identification parameter is a Browser ID.

12. A computer readable medium containing program instructions for creating a computer identifier in the course of an online transaction comprising the steps of:

receiving, from an online customer's computer, at least one of either a personal or non-personal identification parameter;

capturing, from the clock of said customer's computer, said computer's local time;

capturing, from the clock of said website's server computer, said server computer's local time;

creating and storing a delta of time parameter based upon the difference between said customer's computer's local time and said server computer's local time; and

uniquely identifying said customer with customer identification customer identification data comprising said delta of time parameter and said at least one of either of said personal or non-personal identification parameter.

13. The computer readable medium of Claim 12 further including the step of:

receiving and storing, from said customer, personal identification information relating to said transaction.

14. The computer readable medium of Claim 12 further including the step of:

communicating to the website operator an indication as to whether a second online transaction may be fraudulent because of the similarity existing between the stored customer identification data and the new customer's identification data..

15. The computer readable medium of Claim 14 further including the step of:

blocking said second online transaction based upon said indication as to whether a second online transaction may be fraudulent.

16. The computer readable medium of Claim 14 further including the step of:

communicating to said customer the status of said second online transaction based upon the similarity of said stored customer identification data and the new customer's identification data.

17. A computer readable medium as claims in claim 11 wherein said non-personal computer identification parameter is a Browser ID.

18. A computer readable medium containing program instructions for detecting likelihood of fraud in an online transaction comprising the steps of:

creating a first computer identifier in the course of an online transaction comprising the steps of Claim 1;

creating at least one additional computer identifier in the course of an additional online transaction comprising the steps of Claim 1;

utilizing a matching routine to compare said first computer identifier with said at least one additional computer identifier; and

deciding as to whether the online transaction is fraudulent, not fraudulent or requires further consideration

based on the similarities between said first computer identifier and said at least one additional computer identifier.